UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/932,982	08/21/2001	Todd Lagimonier	003636.0115	6823

7590 04/05/2005

MANELLI DENISON & SELTER PLLC
ATTN: William H Bollman
2000 M Street NW
Suite700
Washington, DC 20016

EXAMINER	
SCHUBERT, KEVIN R	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 04/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/932,982	LAGIMONIER, TODD	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-43 have been considered.

Title

The title is too long. The examiner suggests that the title be changed to "Efficiently Handling Cryptographic Messages Containing Nonces". Appropriate correction is suggested.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-43 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier, U.S. Patent No. 5,970,143.

As per claims 1,10, and 19, the applicant describes a method of processing messages comprising the following limitations which are met by Schneier:

a) comparing a nonce value of a received message with a largest nonce value yet seen (Col 16, lines 9-16);

b) comparing said nonce value to an acceptance window in response to said nonce value not exceeding said largest nonce value yet seen (Col 16, lines 17-32);

c) rejecting said received message in response to said nonce value falling outside said acceptance window (Col 16, lines 17-32);

The largest nonce value yet seen is the stored sequence number. Also, in Schneier's system the acceptance window is a time-based history log which stores unexpired nonces that

have been received. If the nonce value is not received within the prescribed time limitation, it is rejected as not being fresh. If a message is not fresh it is a replay attack.

Regarding claim 10, the communication interface is the modem (20 of Fig 2; Col 11, lines 56-58). The controller is the processor of the central computer.

As per claim 28, the applicant describes a system for processing messages in a peer-to-peer configuration comprising the following limitations:

a) a first peer configured to provide secure communication (14 of Fig 2);

b) a second peer configured to provide said secure communication (12 of Fig 2);

c) a secure communication module configured to be executed by said first peer and second peer, wherein said secure communication module is configured to:

i) compare said nonce value to a filter in response to a nonce value of a received packet not exceeding a largest nonce value yet seen (Col 16, lines 24-32);

ii) compare said nonce value to a replay mask (Col 16, lines 24-32);

iii) accept said received packet in response to said comparison of said nonce value and said replay mask being false (Col 16, lines 24-32);

The secure communication module is the secure process which takes place between the first peer, which performs the part of the secure communication module of obtaining a random number and incorporating it in an authentication outcome message (AOM), and a second peer which provides the random number and performs steps i), ii), and iii) above.

The filter is the same as the acceptance window and is comprised of a time limit of acceptance and unexpired messages within that time limit of acceptance which are replay masks to prevent the same nonce from being sent twice. If the nonce is not the largest nonce value yet seen and the time associated with the nonce is within a certain acceptable time limit, it is compared to unexpired messages within the time limit and accepted if the nonce value is not equal to a replay mask value already received.

As per claim 36, the applicant describes an interceptor device for processing messages comprising the following limitations:

a) a network interface (20 of Fig 2; Col 11, lines 56-58);

b) an expected sequence register configured to enumerate an expected sequence number of a packet received from a second network device (Col 16, lines 9-16);

c) a memory configured to store a replay mask (Col 16, lines 24-32);

d) a controller, wherein said controller is configured to:

i) compare said nonce value to a filter in response to a sequence number of a received packet via said network interface does not exceed a largest sequence number yet seen retrieved from said expected sequence register (Col 16, lines 24-32);

ii) compare said sequence number to said replay mask retrieved from said memory (Col 16, lines 24-32);

iii) accept said received packet in response to said comparison of said sequence number and said replay mask is false (Col 16, lines 24-32);

The controller is the processor of the central computer.

As per claims 2,3,11,13,20,21,29, and 37, the applicant discloses the method of claims 1,10,19,28, and 36, which are met by Schneier (see above), further comprising the following limitation which is also met by Schneier:

Designating said nonce value as a nonce value seen in response to said nonce value exceeding said largest nonce value yet seen (Col 16, lines 9-16);

As disclosed by Schneier, "The central computer stores the most recent sequence number in memory" (Col 16, lines 13-14).

As per claims 4,12,22,30, and 38, the applicant discloses the method of claims 1,10,19,28, and 36, which are met by Schneier (see above), further comprising the following limitation which is also met by Schneier:

Adjusting an acceptance window based on said nonce value in response to said nonce value exceeding said largest nonce value yet seen (Col 16, lines 24-32);

The acceptance window is a log of nonces which have been received within a prescribed amount of time. The acceptance window is used to determine a replay attack through two methods: 1) if the nonce received has a time earlier than the acceptance window allows and 2) if the nonce received has already been received and is stored in the acceptance window.

If the nonce received has a value exceeding the largest nonce value yet seen and is accepted as a valid nonce, it is stored in the database of nonces received. The acceptance window is adjusted because the acceptance window will no longer allow the nonce that has just been placed in it.

As per claims 5,7,14,16,23,25,32,34,40, and 42, the applicant describes the method of claim 1,6,10,16,19,24,28,33,36, and 41, which are met by Schneier (see above), with the following limitation which is also met by Schneier:

Designating said received message as a replay attack (Col 16, lines 17-32);

If the acceptance window determines that a message either 1) has a time earlier than the acceptance window allows or 2) has a nonce which has already been received and stored in the acceptance window, the message is determined to not be fresh. If a message is not fresh, it is a replay attack.

As per claims 6,8,15,17,24,26,33, and 41, the applicant describes the method of claims 1,10,19,28, and 36, which are met by Schneier (see above), with the following limitation which is also met by Schneier:

a) comparing said nonce value to a window mask value in response to said nonce value falling within said acceptance window (Col 16, lines 24-32);

b) rejecting said received message in response to an outcome of said comparison of said nonce value to said window mask value being true (Col 16, lines 24-32);

If the nonce value has a time which falls within the acceptance window, it is compared to window mask values to determine if the nonce has already been used. If the nonce value has already been used, the message is rejected. If the nonce has not already been used, the message is accepted.

As per claims 9,18, and 27, the applicant describes the method of claims 8,17, and 26, which are met by Schneier (see above), with the following limitation which is also met by Schneier:

Designating said nonce value as a nonce value seen (Col 16, lines 24-32);

As disclosed by Schneier, "The central computer maintains a database of all random numbers received from the game computers" (Col 16, lines 26-27).

As per claims 31 and 39, the applicant describes the system according to claims 28 and 36, which are met by Schneier (see above), with the following limitation which is also met by Schneier:

Wherein said secure communication module is further configured to reject said received packet in response to said nonce value falling outside said filter (Col 16, lines 17-32);

The nonce value falls outside a filter and is rejected as a replay attack if the nonce's associated time is prior to the acceptable time of the filter.

As per claims 35 and 43, the applicant describes the system according to claims 28 and 36, which are met by Schneier (see above), with the following limitation which is also met by Schneier:

Wherein said secure communication module is further configured to reject said received packet in response to said nonce value fails to fall within said filter and said secure communication module is further configured to designate said received packet as part of a replay attack (Col 16, lines 17-32).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER